# هک چیست و چگونه انجام می‌شود؟


## تاریخچه هک

عمر هک (Hacking) به عنوان بخشی از پردازش و سیستم‌های پردازشی، به ۵ دهه می‌رسد و عناوین و بخش‌های مختلفی دارد. در سال ۱۹۶۰ در MIT اولین هک اتفاق افتاد و در همان زمان اصطلاح هکر به وجود آمد.

## هک چیست؟

هک یعنی چه؟ هک در واقع کاری است که برای پیدا کردن نقاط ورودیِ ممکن در سیستم‌های کامپیوتری و یا شبکه‌های کامپیوتری انجام می‌شود و در نهایت رخنه و ورود، اتفاق می‌افتد Hacking .معمولا برای پیدا کردن راه دسترسی البته از نوع دسترسی غیرمجاز به سیستم‌ها و شبکه‌های کامپیوتری انجام می‌شود. عموما هدف از هک، یا صدمه رساندن به سیستم‌ها است یا دزدیدن اطلاعات موجود در سیستم.

اما هک می‌تواند وجهه قانونی هم داشته باشد و آن زمانی است که از هک برای پیدا کردن نقاط ضعف سیستم‌های شبکه و کامپیوتری استفاده می‌شود. در واقع هک با هدف تست انجام می‌شود. این نوع هک را Ethical Hacking (هک اخلاقی) می‌نامیم. در این محتوا سعی داریم مفاهیم مختلفی از Ethical Hacking را بیان کنیم.

## توصیه های امنیتی برای جلوگیری از هک شدن

با رعایت نکات زیر تا درصد بالایی جلوی هک شدن گرفته می‌شود:

1. استفاده از فایروال در سطح سیستم کامپیوتری و شبکه
2. استفاده از نرم افزارهای معتبر
3. استفاده از ابزارهای مانیتورینگ برای شبکه و سرورها
4. آپدیت سیستم و Firmware و نرم افزارهای نصب شده
5. استفاده از سیستم عامل و نرم افزارهای تست و تایید شده
6. استفاده از سخت افزارهای معتبر و قطعات اورجینال از شرکت های معتبر

7. نصب و آپدیت آنتی ویروس

## هکر کیست؟

هکر یعنی چه؟ به متخصص کامپیوتری که کار هک کردن را انجام می‌دهد هکر (Hacker) گفته می‌شود. هکر در واقع به دنبال اطلاعاتی است که بفهمد سیستم‌ها چگونه کار می‌کنند و سپس بازی آغاز می‌شود.

## انواع هک چیست؟

بر اساس اینکه چه چیزی هک می‌شود، می‌توان هک را به دسته‌ها و انواع مختلفی تقسیم کرد. در ادامه انواع هک را معرفی می‌کنیم:

### Website Hacking - هک وب سایت

هک وب سایت یعنی به دست گرفتن غیرمجاز کنترل روی وب سایت و نرم افزارهای مربوط به آن مانند دیتابیس و اینترفیس‌های دیگر. خواندن مطلب" روش های جلوگیری از هک وب سایت ها "در زمینه امنیت مفید است.

### Network Hacking - هک شبکه

هک شبکه یعنی جمع‌آوری اطلاعات درباره شبکه با استفاده از ابزارهایی مانندTelnet ، NS lookup، Ping، Tracert، Netstatو غیره. این کار با هدف آسیب رساندن به سیستم شبکه و از کارانداختن آن انجام می‌شود.

پیشنهاد مطالعه: شبکه چیست ؛ تعریف کامل انواع شبکه و توپولوژی های آن

### Email Hacking - هک ایمیل

هک ایمیل شامل دسترسی غیرمجاز به اکانت ایمیل و استفاده از آن بدون اجازه مالک آن است. مطلب" جلوگیری از هک ایمیل و بالا بردن امنیت آن "در این زمینه نکات بسیار کاربردی و مهمی ارایه می‌دهد.

### Ethical Hacking - هک اخلاقی

با هدف تست سیستم شبکه و کامپیوتر است و شامل یافتن نقاط ضعف این سیستم‌ها است .در نهایت هم این نقاط ضعف، اصلاح می‌شود.

### Password Hacking - هک رمز عبور

هک کردن رمز عبور و پسورد شامل ریکاور کردن پسوردها از اطلاعاتی است که یا روی سیستم‌ها ذخیره شده یا در تراکنش‌ها استفاده شده است.

### Computer Hacking - هک کامپیوتر

هک کردن کامپیوترها شامل دزدیدن رمز عبور و ID با استفاده از روش‌های هک است و هکر با این اطلاعات، اقدام به دسترسی غیرمجاز به سیستم پردازشی می‌کند.

پیشنهاد مطالعه: سرور چیست؟

## مزایای هک چیست؟

هک در مواردی که در ادامه آمده، نه تنها ضرر ندارد بلکه از مزایای هک محسوب می‌شود:

1. ریکاور کردن اطلاعات گمشده مخصوصا وقتی پسورد تان را فراموش کرده‌اید.
2. انجام تست نفوذ برای بالا بردن امنیت شبکه و کامپیوتر
3. قرار دادن مقیاس‌های پیشگیرانه به میزان کافی
4. داشتن سیستم‌های کامپیوتری‌ای که جلوی هکرهای بدجنس را از دسترسی بگیرند.

## معایب هک چیست؟

با وجود تمام مزایایی که برای Hacking برشمردیم، هک می‌تواند خطرناک باشد و با مقاصد خرابکاری انجام شود که نتیجه آن به شرح زیر است:

1. رسوخ امنیتی به شکل انبوه
2. دسترسی غیرمجاز به سیستم‌ها برای به دست آوردن اطلاعات شخصی
3. تجاوز به حریم شخصی
4. مختل کردن سیستم‌ها
5. حمله Denial of Service یاDoS
6. حمله به سیستم‌ها

## هک چگونه صورت می گیرد؟

هکری چیست؟ هکرها معمولا به دو شیوه به سامانه‌های کاربران و زیرساخت‌های ارتباطی حمله می‌کنند:

۱ .مدل اول الگویی ثابت و شناخته شده دارد : هکر یا هکرها بدافزارهایی را تولید می‌کنند و به روش‌های مختلفی همچون تزریق کد، ضمایم آلوده ایمیلی یا سایت‌های مخرب بدافزارها را به سامانه قربانیان وارد می‌کنند. در این شیوه بدافزار به سامانه قربانیان وارد می‌شود، بخش‌های مختلف سامانه را آلوده می‌کند و خساراتی به سامانه‌ها وارد می‌کند.

در مقیاس وسیع‌تر، بدافزارها به شبکه‌های سازمانی نفوذ می‌کنند و به سرقت اطلاعات یا دستکاری اطلاعات می‌پردازند.در هر دو حالت، تمامی این فرآیندهای مخرب توسط بدافزاری انجام می‌شود که کدهای آن از قبل نوشته شده و پس از انتشار هکر نمی‌تواند تغییری در بدافزار به وجود آورد مگر آن‌که نسخه دیگری از بدافزار را طراحی کند و مراحل آلوده‌سازی را یکبار دیگر تکرار کند.

۲ .مدل دوم، الگویی متغیر دارد و انعطاف‌پذیری بیشتری در اختیار هکرها قرار می‌دهد، به‌طوری که هکرها زیرساختی را برای حمله به اهداف مختلف آماده می‌کنند. در این حمله، هکرها زیرساختی متشکل از هزاران یا صدها هزار کامپیوتر آلوده را آماده می‌کنند و هنگامی که شرایط مهیا شد از این زیرساخت غیر متمرکز برای حمله به وب‌سایت‌ها یا شرکت‌های بزرگ استفاده می‌کنند. یکی از کاربردهای اصلی این زیرساخت در حمله‌های منع سرویس توزیع‌شده (DDoS) است که با هدف از دسترس خارج کردن سرویس‌های کاربردی یک وب‌سایت به مرحله اجرا در می‌آید. برای آشنایی با حمله دیداس و انواع و نحوه پیاده سازی آن مقاله" حمله ddos چیست و چگونه از حملات دیداس جلوگیری کنیم "را مطالعه کنید. کاربردهای این زیرساخت تهاجمی که بات نت (BotNet) نام دارد فراتر از حمله‌های منع سرویس توزیع شده و قادر به انتشار اخبار جعلی یا حتا استخراج رمزارزها است.

## هدف از هک کردن چیست؟

همان طور که گفته شد، هک کردن می‌تواند با اهداف مثبت و یا منفی انجام شود. دلایلی که افراد، اقدام به هک کردن می‌کنند به شرح زیر است:

1. تفریح

2. خودنمایی
3. دزدیدن اطلاعات مهم
4. آسیب زدن به سیستم
5. تجاوز به حریم شخصی
6. اخاذی
7. تست امنیت سیستم

پیشنهاد مطالعه: راهکارهای تامین امنیت شبکه

## انواع هکرها بر اساس هدف هکر

در این قسمت می‌خواهیم هکرها را دسته‌بندی کنیم. این دسته‌بندی بر اساس هدف هکر از هک کردن سیستم است. در ادامه انواع هکرها را از این منظر معرفی می‌کنیم:

انواع هکرها بر اساس هدف هکر

### 1. هکرهای کلاه سفید(White Hat Hacker)

هکرهای کلاه سفید را با عنوان Ethical Hacker هم می‌شناسیم. این هکرها نه تنها هرگز به سیستم‌ها آسیب نمی‌زنند بلکه سعی دارند نقاط ضعف سیستم شبکه و کامپیوتر را با تست‌های پیشگیرانه و ارزیابی‌های آسیب‌پذیری پیدا کنند.

Ethical Hackیا هک اخلاقی، غیرقانونی نیست و یکی از سِمت‌هایی است که در صنعت IT وجود دارد. شرکت‌های بسیاری هستند که اتیکال هکرها را استخدام می‌کنند تا تست‌های پیشگیرانه و ارزیابی‌های آسیب‌پذیری را انجام دهند.

### 2. هکرهای کلاه سیاه(Black Hat Hacker)

هکرهای کلاه سیاه را با عنوان Cracker هم می‌شناسیم. این هکرها به منظور دسترسی غیرمجاز به سیستم و آسیب زدن به آن و یا دزدیدن اطلاعات، اقدام به هک می‌کنند.

هک کلاه سیاه همواره غیرقانونی است چرا که اهداف شومی در بر دارد که شامل دزدیدن اطلاعات شرکت‌ها، تجاوز به حریم شخصی، آسیب زدن به سیستم و بلاک کردن ارتباطات داخل شبکه است.

### 3. هکرهای کلاه خاکستری(Grey Hat Hacker)

هکرهای کلاه خاکستری، مخلوطی از هکرهای کلاه سفید و هکرهای کلاه سیاه هستند. آنها بدون اهداف شرورانه هستند اما هک برای آنها جنبه فان و تفریح دارد، و یا ضعف امنیتی سیستم و شبکه را پیدا می‌کند که البته بدون اجازه صاحبان آن انجام می‌شود.

هدف هکرهای کلاه خاکستری این است که صاحبان سیستم‌ها را از ضعف‌ها مطلع کنند و مورد سپاسگزاری قرار گیرند و یا هدیه‌ای دریافت کنند.

**مطالعه مقالات" روش های جلوگیری از هک کامپیوتر و لپ تاپ "و" جلوگیری از هک شدن گوشی موبایل و اکانت های شبکه های اجتماعی "پیشنهاد می‌شود.**

## انواع هکرها بر اساس چگونگی هک کردن

در این قسمت می‌خواهیم دسته‌بندی دیگری برای هکرها ارایه کنیم. این دسته‌بندی بر این اساس است که هکر چه چیزی را هک می‌کند و چگونه هک می‌کند. در ادامه انواع هکرها را از این منظر معرفی می‌کنیم:

انواع هکرها بر اساس چگونگی هک کردن

### 1. هکرهای کلاه قرمز(Red Hat Hacker)

هکرهای کلاه قرمز، مخلوطی از هکرهای کلاه سفید و هکرهای کلاه سیاه هستند که فعالیت آنها در زمینه هک کردن سیستم‌های دولتی، مراکزی که از نظر امنیتی سطح بالایی دارند، و در کل هر آنچه را که شامل اطلاعات حساس است را هک می‌کنند.

### 2. هکرهای کلاه آبی(Blue Hat Hacker)

هکرهای کلاه آبی کسانی هستند که دقیقا خارج از گود امنیت کامپیوتر فعالیت می‌کنند و در زمینه پیدا کردن باگ های سیستم مشاوره می‌دهند. آنها به دنبال روزنه‌هایی هستند که احتمال دارد مورد سواستفاده قرار گیرند و سعی دارند این گپ‌ها را ببندند. مایکروسافت اصطلاح Blue Hat را برای ارایه یک سری موارد امنیتی استفاده می‌کند.

### 3. هکرهای الیت(Elite Hacker)

در بین هکرها موقعیت اجتماعی دارد که بهترین مهارت‌ها را توضیح می‌دهند و اخیرا هم تمام رخنه‌ها توسط این گروه از هکرها کشف شده است.

### 4. هکرهای اسکریپت(Script Kiddie)

هکرهای اسکریپتی هیچ مهارتی در رخنه به سیستم ندارند و این کار را فقط با استفاده از ابزارهایی که دیگران نوشته‌اند انجام می‌دهند.

### 5. هکرهای مبتدی یا کلاه سبز(Neophyte / Green Hat)

هکرهای مبتدی یا کلاه سبز کسانی هستند که در زمینه هک، تازه‌کار است و تقریبا هیچ تجربه و دانشی برای کار روی تکنولوژی و هک ندارند.

### 6. هکرهایHacktivist

هکتیویست، هکری است که از تکنولوژی استفاده می‌کند تا پیام سیاسی یا مذهبی یا اجتماعی یا ... را اعلام کند. این هکرها معمولا حمله DoS و یا هک وب سایت ها را انجام می‌دهند.

انواع هکرها بر اساس چگونگی هک کردن

**مطالعه مقالات" معنی Footprint در دنیای تکنولوژی چیست؟ "پیشنهاد می‌شود.**

## مهارت‌ها و ویژگی‌های شخصیتی لازم برای هکرها

هک کردن سیستم‌های کامپیوتری علاوه بر اینکه علم است هنر هم هست. و برای اینکه هکر ماهری شوید باید دانش زیادی کسب کنید. علاوه بر این باید دانش خود را آپدیت نگه دارید و جدیدترین تکنولوژی‌ها و تکنیک‌های رخنه را بررسی کنید.

هکر باید کارشناس سیستم‌های کامپیوتری باشد، برنامه‌نویس بسیار قوی و دارای مهارت‌های شبکه کامپیوتری باشد.

هکر باید صبر و پشتکار خوبی داشته باشد تا بتواند بارها و بارها کاری را تست کند و منتظر گرفتن نتیجه باشد.

هکر باید به اندازه کافی باهوش باشد تا شرایط را درک کرده و مدل تفکری دیگران را بداند تا بتواند رخنه‌ها را تشخیص دهد.

هکرِ خوب، مهارت و قدرت حل مساله در سطح بالا را دارد.

پیشنهاد مطالعه: امنیت سایبری چیست و چطور می توان آن را تامین کرد؟

## مهارت‌ها و تخصص‌های لازم برای هکرها

1. مدرک علوم کامپیوتر، گواهی نامه های آشنایی با سخت افزارها و نرم افزارها
2. برنامه نویسی به مدت چند سال و سپس داشتن جایگاه پشتیبانی فنی
3. گواهی نامه های شبکه شامل Network+ وCCNA
4. گواهی نامه های امنیت شامل Security+ و CISSP وTICSA
5. تجربه کار در جایگاه مهندس شبکه و ادمین سیستم
6. یادگیری پیوسته در زمینه امنیت کامپیوتر و به کارگیری آن برای امن کردن سیستم‌های شبکه و کامپیوتری در جایگاه مهندس امنیت شبکه
7. مطالعه و یادگیری در زمینه‌های زیر:

- Trojan horses
- Backdoors
- Viruses
- Worms
- Denial of Service (DoS) Attacks
- SQL Injection
- Buffer Overflow
- Session Hijacking
- System Hacking